mailguard

BASIC CONFIGURATION GUIDE

WebGuard 2.0
Secure Web-Browsing Management

Revision 3.0

mailguard

1.0   Introduction

WebGuard brings many benefits to your clients' valuable network – such as a virus free browsing experience and visibility into the browsing habits of employees – but how easy is it to setup for your client?

There are three main components – WebGuard Console setup, Network Setup and Network User setup. We have also included some tips on policies, setup and roaming users.

Step 1: Basic WebGuard Console Setup

➔   Receive welcome email

➔   Logon to the Unified console

➔   Go to Configure>WebGuard>Networks

- •   'Add' a network (or mulitple networks if you have multiple internet links
- •   Name network (ie/ Name after geo location)
- •   Enter static public IP Address - In the 'Network Access' field
- •   Leave NTLM as the default authentication method
- •   Click 'Submit'
- •   'Edit' your Network'
- •   Click 'Proxy Preference'
- •   'Add' proxy servers (select a least 3 for maximum redundancy)

Step 2: Network Setup

➔   Test ports 9002 & 9003 for connectivity outbound for any host

- •   Ie/ In Command Prompt - telnet www.webguard.com.au 9003

If the client has an Intranet, put the host name into the 'URL Routing' list of each network (e.g. http://myintranet.com/)

Step 3: Network User Setup

To enable WebGuard with Active Directory

➔   Use AD to push script that forces the auto configuration script to be enforced on all WG protected computers.

Auto configuration script is – http://www.webguard.com.au:9003/proxy.pac

To enable WebGuard without Active Directory

On each computer to be protected by WebGuard

➔   Open Internet Explorer

- Click Tools, then Internet Options, Connections, Lan Settings
- "Check" Use Automatic configuration script
- Enter - http://www.webguard.com.au:9003/proxy.pac
- Close/restart IE browser
- Test – go to www.whatismyip.com
- Should not see their public IP address but the WebGuard proxy server address instead.

➔   Open Firefox

- Click Tools, then Options, Advanced tab, Network, Settings
- "Check" Automatic proxy configuration URL:
  Enter - http://www.webguard.com.au:9003/proxy.pac
- Click reload button
- Test: Go to www.whatismyip.com
- Should not see their public IP address but the WebGuard proxy server address instead.

Roaming Users

Because roaming users are on a dynamic IP address, the WebGuard system requires authentication. Each time the browser is opened a login prompt will appear.

After Computer User Setup steps have been followed.

➔   To enable a roaming user to be protected by WebGuard

- Click on Configure>Users in the console
- Click 'Add' button in the Users section
- Add a First Name and Surname and click 'Submit'
- Click 'WebGuard Username' on the right
- Click 'Add'
- Specify a unique Username and Password and then click 'Submit' (it's a good idea to add an email address to this user for easy identification)

When a roaming user connects through known static IP address they will be identified as a regular network user. Nb: To avoid being billed twice for 1 user (NTLM & Digest) you can assign a password to an existing NTLM created user which will then double as a Digest user.

Setup Tips

- The daily welcome message will appear once a day when the user connects to WebGuard. To turn this off this must be requested via the MG Service Desk at any point after provisioning.
- If the client has a dynamic IP address then choose the 'Digest' method of authentication in the console setup.

- If the Client has a static IP address then always choose the 'NTLM' method of authentication in the console setup (unless Digest login is preferred).

- During setup also make sure a daily, weekly or monthly report is setup to go to a key member of the client – this will help validate the service to the client.

Policy Tips

These are suggested policies to setup as a standard for your clients when you are setting up their console.

- Setup AV policy for company wide.

- Setup Offensive Category policy – company wide
  - Pornography Site
  - Sexual Orientation Site
  - Hate Site/Hate Speech Site
  - Child Pornography Site
  - Nudism and Naturism Site
  - Gore Site
  - Violence Site

(These are suggestions only and we recommend you consult the client for further instruction.)

- Setup policy to not scan for virus based on object types – company wide
  - Video file/Audio file/Shockwave Flash

Help & Support:

For any advice on a unique setup always call the MailGuard Service Desk.
They will be more than happy to assist in your clients WebGuard setup.

Contact:

Head Office:

68-72 York Street,
South Melbourne
Victoria, 3205
Australia

Freecall: 1300 30 44 30 within Australia/NZ
Tel: +61 3 9694 4444 from overseas
Fax: +61 3 9011 6110

Technical Support:

Freecall: 1300 30 65 10 within Australia/NZ
                 Mon- Fri: 8.30am - 5.30pm AEST (Emergency, 24/7)
Tel: +61 3 9694 4444 from overseas
Fax: 1300 30 75 20
Email: support@mailguard.com.au

Sales:

Freecall: 1300 30 44 30 within Australia/NZ
Tel: +61 3 9694 4444
Email: sales@mailguard.com.au

www.mailguard.com.au